SOPHOS
Security made simple.

Sophos Mobile as a Service

Guida di avvio

Versione prodotto: 8

Sommario

1 Informazioni sulla guida

Questa guida indica come impostare Sophos Mobile as a Service come sistema di gestione dei dispositivi.

Ulteriori informazioni sono disponibili nella Guida in linea per amministratori di Sophos Mobile.

Questa guida si concentra sulle piattaforme Android e iOS, in quanto si tratta delle piattaforme più comunemente utilizzate. Le impostazioni qui descritte possono essere applicate in modo simile anche agli altri sistemi operativi supportati.

2 Passaggi chiave

Per cominciare ad utilizzare Sophos Mobile:

1. Reimpostare la password, accedere a Sophos Mobile Admin e cambiare il nome utente dell'amministratore.
2. Richiesto: Attivare le licenze Mobile Advanced per gestire le app Sophos Mobile Security, Sophos Secure Workspace e Sophos Secure Email.
3. Verificare i dati relativi alla licenza.
4. Configurare le impostazioni personali, i criteri per la password da applicare agli account amministratore, i dati di contatto del supporto tecnico, e le impostazioni per il portale self-service.
5. Caricare un certificato per l'Apple Push Notification service per gestire i dispositivi iOS.
6. Richiesto: Impostare un proxy di EAS standalone per filtrare il traffico e-mail proveniente dai dispositivi gestiti e dirigerlo verso un server di posta elettronica.
7. Richiesto: Configurare l'interfaccia per sistemi di Network Access Control di terzi.
8. Creare criteri di conformità.
9. Creare gruppi di dispositivi.
10. Configurare i dispositivi.
11. Aggiornare le impostazioni del portale self-service.
12. Configurare la gestione degli utenti
13. Se si utilizza la gestione degli utenti interni: Aggiungere utenti sia creandoli che caricando elenchi di utenti.
14. Se si utilizza la gestione degli utenti esterni: Configurare la connessione alla directory di LDAP.
15. Effettuare un test della registrazione nel portale self-service.

3 Modifica della password

Per questioni di sicurezza, si consiglia di reimpostare la password prima di effettuare l'accesso a Sophos Mobile Admin per la prima volta.

1. Aprire Sophos Mobile Admin nel browser web.
2. Nella finestra di dialogo di **Accesso**, cliccare su **Password dimenticata?**.
3. Nella finestra di dialogo **Reimposta password**, inserire le informazioni relative a **Cliente** e **Utente** reperibili nell'e-mail ricevuta per l'attivazione dell'account di Sophos Mobile as a Service, quindi cliccare su **Reimposta password**.
   Una volta portata a termine questa procedura, riceverà un'e-mail contenente un link che le consentirà di reimpostare la password.
4. Cliccare sul link per aprire la finestra di dialogo **Cambia password**.
5. Inserire la nuova password, e cliccare su **Cambia password**.

   La password è stata modificata. Ricordarsi di utilizzare questa password al prossimo accesso alla console.

Nota

Si consiglia di modificare i criteri della password per implementare password più sicure, ad esempio richiedendo un numero minimo di caratteri minuscoli, maiuscoli o speciali. Vedere Configurazione dei criteri delle password (pagina 8).

4 Modifica del nome di accesso

Per motivi di sicurezza, si consiglia di cambiare il nome di accesso dell'amministratore una volta effettuato il primo accesso a Sophos Mobile Admin.

1. Nella barra laterale del menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Amministratori**.
2. Nella pagina **Mostra amministratori**, cliccare sul triangolo blu accanto al nome di accesso, e successivamente su **Modifica**.
3. Nella pagina **Modifica amministratore**, inserire un valore diverso nel campo **Nome di accesso**.
4. Richiesto: Modificare i valori degli altri campi:
   - **Nome**
   - **Cognome**
   - **Indirizzo e-mail**
5. Cliccare su **Salva**.

I dettagli dell'account sono stati modificati. Ricordarsi di utilizzare il nuovo nome di accesso al prossimo accesso a Sophos Mobile Admin.

5 Attivazione di licenze Mobile Advanced

Con le licenze Mobile Advanced, è possibile utilizzare Sophos Mobile per gestire le app Sophos Mobile Security, Sophos Secure Workspace e Sophos Secure Email.

Le licenze Mobile Advanced vengono attivate dalla Sophos Mobile Admin:

1. Nella barra laterale del menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Impostazione del sistema**.
2. Sotto la scheda **Licenze**, inserire la chiave di licenza all'interno del campo **Chiave di licenza Advanced** e cliccare su **Attiva**.

Una volta attivata la chiave, verranno visualizzati i dettagli della licenza.

6 Verifica delle licenze

Sophos Mobile utilizza un sistema di licenze basato sul numero di utenti. Una sola licenza è valida per tutti i dispositivi assegnati a un utente. I dispositivi non assegnati ad alcun utente richiedono invece una licenza ciascuno.

Per verificare le licenze disponibili:

1. Nella barra laterale del menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Impostazione del sistema**.
2. Nella pagina **Impostazione del sistema**, cliccare sulla scheda **Licenze**.

Verranno visualizzate le seguenti informazioni:

- **Numero massimo di licenze**: Il numero massimo di utenti dei dispositivi (e dispositivi non assegnati) che è possibile gestire.
- **Licenze utilizzate**: Numero di licenze in uso.
- **Valido entro**: La data di scadenza della licenza.

Nel caso di domande o dubbi sulle informazioni relative alla licenza che sono visualizzate, contattare il proprio rappresentante commerciale Sophos.

7 Configurazione delle impostazioni

Configurare le seguenti impostazioni:

- Impostazioni personali, per esempio le piattaforme che si desidera gestire
- Criteri password
- Dati di contatto del supporto tecnico
- Impostazioni del portale self-service

7.1 Configurazione delle impostazioni personali

Per utilizzare Sophos Mobile Admin in maniera più efficace, è possibile personalizzare l'interfaccia utente in modo tale da visualizzare solo le piattaforme in uso.

Nota
Configurando le piattaforme viene modificata solamente la vista degli utenti al momento collegati, da cui non è possibile disattivare alcuna funzione.

1. Nella barra laterale del menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Generale**, e successivamente cliccare sulla scheda **Privato**.
2. Configurare le seguenti impostazioni:

Opzione	Descrizione
Lingua	Selezionare la lingua in cui si desidera visualizzare Sophos Mobile Admin.
Fuso orario	Selezionare il fuso orario in cui vengono indicate data e ora.
Unità di misura	Selezionare le unità di misura per i valori di lunghezza (**Metriche** or **Imperiali**).
Righe per pagina nelle tabelle	Selezionare il numero massimo di righe per tabella che si desidera visualizzare in ciascuna pagina.
Mostra dettagli dispositivo estesi	Selezionare questa casella di spunta per visualizzare tutte le informazioni disponibili sul dispositivo. Le schede **Proprietà personalizzate** e **Proprietà interne** verranno aggiunte alla pagina **Mostra dispositivo**.
Piattaforme attive	Selezionare le piattaforme che si desidera gestire: • **Android** • **Android Things** • **iOS** • **Windows Mobile** (include i sistemi operativi Windows Phone 8.1 e Windows 10 Mobile) • **Windows** • **Windows IoT** L'interfaccia utente di Sophos Mobile Admin cambierà in base alle piattaforme selezionate. Verranno visualizzate solamente

Opzione	Descrizione
	le viste e le funzionalità che riguardano le piattaforme selezionate.

3. Cliccare su **Salva**.

7.2 Configurazione dei criteri delle password

Per implementare la protezione delle password, configurare criteri delle password per gli utenti di Sophos Mobile Admin e del Portale self-service.

Nota
I criteri delle password non sono applicabili agli utenti provenienti da una directory LDAP esterna.

1. Nella barra laterale del menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Generale**, e successivamente cliccare sulla scheda **Criteri password**.
2. Sotto **Regole**, è possibile definire requisiti per le password, come ad es. la quantità minima di caratteri maiuscoli, minuscoli o numerici che una password deve contenere per essere considerata valida.
3. Sotto **Impostazioni**, configurare le seguenti impostazioni:
   a) **Intervallo di modifica password (giorni)**: Inserire il numero di giorni dopo il quale una password verrà ritenuta scaduta (tra `1` e `730`), oppure lasciare il campo vuoto per disattivare la scadenza della password.
   b) **Numero di password precedenti da non riutilizzare**: Selezionare un valore compreso tra `1` e `10`, oppure selezionare `---` per disattivare questa restrizione.
   c) **Numero massimo di tentativi di accesso non riusciti**: Selezionare il numero di tentativi di accesso non riusciti dopo il quale l'account debba essere bloccato (cifra compresa tra `1` e `10`), oppure selezionare `---` per consentire una quantità illimitata di tentativi di accesso non riusciti.
4. Cliccare su **Salva**.

7.3 Configurazione dei dati di contatto del supporto tecnico

Per fornire supporto agli utenti che avessero domande o problemi, potete fornire i dettagli di come contattare il supporto tecnico. Le informazioni qui inserite verranno visualizzate nell'app Sophos Mobile Control e nel portale self-service.

1. Nella barra laterale del menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Generale**, e successivamente cliccare sulla scheda **Contatto tecnico**.
2. Inserire le informazioni relative al supporto tecnico.
3. Cliccare su **Salva**.

7.4 Configurazione delle impostazioni del portale self-service

1. Nella barra laterale del menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Portale self-service**.
   Si aprirà la pagina del **Portale self-service**.
2. Nella scheda **Configurazione**, configurare le impostazioni del portale self-service in base alle proprie esigenze.

   Se a questo punto non si fosse sicuri di quali impostazioni applicare, si consiglia di adoperare le impostazioni predefinite.

   Per una descrizione dettagliata delle impostazioni, cliccare su **?** nell'intestazione della pagina.
3. Nella scheda **Termini di utilizzo**, cliccare su **Modifica** per inserire un testo contenente una declinazione di responsabilità, o un consenso, per il criterio per i dispositivi mobili.

   Questo testo verrà visualizzato all'inizio del processo di registrazione del dispositivo. Gli utenti devono accettare il testo prima di poter effettuare la registrazione.

   Consiglio
   È possibile utilizzare la barra degli strumenti editor per applicare al testo una formattazione HTML di base. Ciò è valido anche per il testo di post-installazione descritto nel passaggio successivo.

4. Opzionale: Nella scheda **Testo di post-installazione**, cliccare su **Modifica** per inserire un testo da visualizzare al completamento della registrazione del dispositivo.

   Il testo può essere utilizzato anche per descrivere qualsivoglia passaggio successivo che l'utente debba svolgere dopo la registrazione.
5. Cliccare su **Salva**.

8 Certificati Apple Push Notification service

Per utilizzare il protocollo Mobile Device Management (MDM) incorporato nei dispositivi iOSe macOS, Sophos Mobile deve utilizzare il servizio Apple Push Notification (APNs) per l'attivazione dei dispositivi.

I certificati APNs sono validi per un anno.

Le sezioni che seguono definiscono i requisiti da soddisfare e le azioni da intraprendere per ottenere l'accesso ai server di APNs con il proprio certificato client.

8.1 Requisiti

Per la comunicazione con Apple Push Notification Service (APNs), occorre autorizzare il traffico TCP in entrata e in uscita dalle seguenti porte:

- Il server di Sophos Mobile deve potersi connettere a `gateway.push.apple.com:2195 TCP (17.0.0.0/8)`
- Ciascun dispositivo iOS dotato solamente di accesso Wi-Fi deve potersi connettere a `*.push.apple.com:5223 TCP (17.0.0.0/8)`

8.2 Creazione di un certificato APNs

1. Nella barra laterale dei menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Impostazione del sistema** e successivamente sulla scheda **APNs**.

   La descrizione di questa scheda indica la procedura dettagliata da seguire per richiedere un certificato da Apple e caricarlo in Sophos Mobile.
2. Nel passaggio **Scaricare la richiesta di firma del certificato**, cliccare su **Scarica richiesta di firma del certificato**.

   Questa operazione salva il file di richiesta di firma del certificato `apple.csr` sul computer locale.
3. Occorre un ID Apple. Anche se si è già in possesso di un ID, si consiglia di crearne uno nuovo da utilizzare esclusivamente per Sophos Mobile. Nel passaggio **Creazione di un ID Apple**, cliccare su **Creare un nuovo ID Apple**.

   Si aprirà una pagina web di Apple nella quale sarà possibile creare un ID Apple per l'azienda.

   Nota

   Conservare le credenziali in un posto sicuro, a cui i colleghi possano accedere. L'azienda avrà bisogno di queste credenziali ogni anno, per rinnovare il certificato.
4. Come riferimento, inserire il nuovo ID Apple nel campo **ID Apple** nella parte alta della scheda **APNs**.

   Ogni anno, al rinnovo del certificato, occorrerà sempre utilizzare lo stesso ID Apple.
5. Nel passaggio **Creazione o rinnovo di un certificato APNs**, cliccare su **Apple Push Certificates Portal**.

Verrà aperto l'Apple Push Certificates Portal.

6. Accedere con il proprio ID Apple e caricare il file di richiesta di firma del certificato `apple.csr`.
7. Scaricare il file `.pem` del certificato APNs e salvarlo nel computer.
8. Nel passaggio **Upload di un Certificato APNs**, cliccare su **Carica certificato** e cercare il file `.pem` ricevuto dall'Apple Push Certificates Portal.
9. Cliccare su **Salva** per aggiungere il certificato APNs a Sophos Mobile.

Sophos Mobile leggerà il certificato e visualizzerà i dettagli del certificato nella scheda **APNs**.

9 Proxy EAS standalone

È possibile impostare un proxy di EAS per controllare l'accesso dei dispositivi gestiti a un server di posta. Il traffico e-mail dei dispositivi gestiti verrà reindirizzato attraverso il proxy specificato. È possibile bloccare l'accesso alle e-mail per i dispositivi, ad esempio nel caso in cui sia presente un dispositivo che viola una regola di conformità.

I dispositivi devono essere configurati in modo da utilizzare il proxy di EAS come server di posta elettronica per le e-mail in entrata e in uscita. Il proxy EAS inoltrerà il traffico al server di posta elettronica solamente se il dispositivo è noto a Sophos Mobile, e se soddisfa i criteri richiesti. Ciò garantisce un livello di sicurezza più elevato, in quanto non occorre che il server di posta sia accessibile da Internet, e può essere raggiunto solamente dai dispositivi autorizzati (configurati correttamente, ad es. seguendo linee guida per il passcode). Inoltre, è anche possibile configurare il proxy di EAS in modo che impedisca l'accesso da dispositivi specifici.

Il proxy di EAS standalone deve essere scaricato e installato separatamente da Sophos Mobile. Comunica con il server di Sophos Mobile attraverso un'interfaccia web HTTPS.

Nota

Poiché macOS non supporta il protocollo ActiveSync, non è possibile utilizzare il proxy di EAS interno o standalone per filtrare il traffico e-mail proveniente dai Mac.

Funzionalità

- Supporto di server di posta elettronica Microsoft Exchange o IBM Notes Traveler multipli. È possibile impostare un'istanza di proxy di EAS per ciascun server di posta.
- Supporto di bilanciatori del carico. È possibile impostare istanze di proxy di EAS standalone su computer diversi, per poi utilizzare un bilanciatore del carico per distribuire tra di esse le richieste del client.
- Supporto dell'autenticazione al client basata su certificato. È possibile selezionare, da un'autorità di certificazione (CA), un certificato dal quale devono essere derivati i certificati client.
- Supporto del controllo dell'accesso alle e-mail tramite PowerShell. In questo scenario, il servizio proxy EAS comunica con il server di posta tramite PowerShell per controllare l'accesso alle e-mail dei dispositivi gestiti. Il traffico e-mail si verifica direttamente tra i dispositivi e i server di posta, senza essere reindirizzato tramite un proxy. Vedere Impostazione del controllo dell'accesso alle e-mail tramite PowerShell (pagina 16).

Nota

Per i dispositivi non iOS, le capacità di filtraggio del proxy EAS standalone sono limitate per via delle specifiche del protocollo di IBM Notes Traveler. Sui dispositivi non iOS, i client di Traveler non inviano l'ID del dispositivo con tutte le richieste. Le richieste senza un ID del dispositivo verranno comunque inoltrate al server di Traveler, anche se il proxy EAS non dovesse essere in grado di verificare che il dispositivo è autorizzato.

9.1 Download del programma di installazione del proxy di EAS

1. Accedere a Sophos Mobile Admin.
2. Nella barra laterale del menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Impostazione del sistema**, e successivamente cliccare sulla scheda **Proxy EAS**.
3. Sotto **Esterno**, cliccare sul link per scaricare il programma di installazione del proxy di EAS.

Il file di installazione verrà salvato nel computer locale.

9.2 Installazione del proxy EAS standalone

Prerequisito:

- Tutti i server di posta richiesti devono essere accessibili. Il programma di installazione del proxy EAS non configurerà le connessioni ai server che non sono disponibili.
- Occorre aver effettuato l'accesso come amministratore sul computer in cui si intende installare il proxy EAS.

> **Nota**
> La Guida alla distribuzione di Server di Sophos Mobile contiene diagrammi schematici per l'integrazione del proxy di EAS standalone nell'infrastruttura aziendale. Si consiglia di leggere le informazioni prima di procedere con l'installazione e la distribuzione del proxy di EAS standalone.

1. Eseguire `Sophos Mobile EAS Proxy Setup.exe` per avviare **Sophos Mobile EAS Proxy - Setup Wizard**.
2. Nella pagina **Choose Install Location**, selezionare la cartella di destinazione e cliccare su **Install** per avviare l'installazione.
   Una volta completata l'installazione, viene avviato automaticamente **Sophos Mobile EAS Proxy - Configuration Wizard**, che fornisce una guida passo dopo passo all'intero processo di configurazione.
3. Nella finestra di dialogo **Sophos Mobile server configuration**, inserire l'URL del server di SMC a cui il proxy di EAS effettuerà la connessione.

   Si consiglia di selezionare anche **Use SSL for incoming connections (Clients to EAS Proxy)** per proteggere la comunicazione tra i client e il proxy di EAS.

   Opzionalmente, selezionare **Use client certificates for authentication** se si desidera che, per l'autenticazione, i client adoperino anche un certificato, oltre alle credenziali del proxy di EAS. Così facendo si aggiunge un ulteriore livello di sicurezza alla connessione.

   Selezionare **Allow all certificates** se il server di Sophos Mobile presenta certificati variabili al proxy di EAS, ad esempio quando esistono diverse istanze di server dietro a un bilanciatore di carico, e ciascuna istanza adopera un certificato diverso. Quando è selezionata questa opzione, il proxy EAS accetterà qualsiasi certificato dal server di Sophos Mobile.

Importante
Poiché l'opzione **Allow all certificates** diminuisce il livello di sicurezza della comunicazione del server, si consiglia vivamente di selezionarla solamente se richiesta dall'ambiente di rete.

4. Se precedentemente è stata selezionata l'opzione **Use SSL for incoming connections (Clients to EAS Proxy)**, verrà visualizzata la pagina **Configure server certificate**. In questa pagina è possibile creare o importare un certificato per l'accesso sicuro (HTTPS) al proxy EAS.

   Nota
   La procedura guidata "SSL Certificate Wizard" può essere scaricata da MySophos e utilizzata per richiedere il certificato SSL/TLS per il proxy di EAS di Sophos Mobile.

   Per informazioni generali sul download dei software Sophos, consultare l'articolo 111195 della knowledge base Sophos.

   - Se ancora non si dispone di un certificato attendibile, selezionare **Create self-signed certificate**.
   - Se si dispone di un certificato attendibile, cliccare su **Import a certificate from a trusted issuer** e selezionare una delle seguenti opzioni dall'elenco:
     - **PKCS12 with certificate, private key and certificate chain (intermediate and CA)**
     - **Separate files for certificate, private key, intermediate and CA certificate**
5. Nella pagina successiva, inserire le informazioni del certificato che riguardano il certificato selezionato.

   Nota
   Nel caso di un certificato autofirmato, occorrerà specificare un server che sia accessibile dai dispositivi client.

6. Se precedentemente è stata selezionata l'opzione **Use client certificates for authentication**, verrà visualizzata la pagina **SMC client authentication configuration**. Su questa pagina è possibile selezionare, da un'autorità di certificazione (CA), un certificato dal quale devono essere derivati i certificati client.

   Quando un client cercherà di effettuare la connessione, il proxy di EAS verificherà se il certificato sia derivato dalla CA specificata in questo campo.
7. Nella pagina **EAS Proxy instance setup**, configurare una o più istanze di proxy EAS.
   - **Instance type**: Selezionare **EAS proxy**.
   - **Instance name**: Un nome che identifica l'istanza.
   - **Server port**: La porta del proxy EAS per il traffico e-mail in entrata. Se viene impostata più di un'unica istanza di proxy, ciascuna di esse dovrà utilizzare una porta diversa.
   - **Require client certificate authentication**: I client di posta devono autentificarsi quando si connettono al proxy EAS.
   - **ActiveSync server**: Il nome o indirizzo IP dell'istanza del server di Exchange ActiveSync a cui si connetterà l'istanza del proxy.
   - **SSL**: La comunicazione tra l'istanza del proxy e il server di Exchange ActiveSync è protetta tramite SSL o TLS (a seconda della compatibilità del server).

- **Allow EWS subscription requests from Secure Email**: Selezionare questa opzione per consentire alla app Sophos Secure Email su iOS di effettuare la sottoscrizione alle notifiche push tramite Exchange Web Services (EWS). Le notifiche push informano il dispositivo quando sono presenti messaggi per Secure Email.

  Nota
  Per impostazione predefinita, il proxy di EAS blocca tutte le richieste rivolte all'interfaccia EWS del server di Exchange; ciò è per questioni di sicurezza. Selezionando questa casella di controllo, verranno autorizzate le richieste di sottoscrizione. Le altre richieste rimarranno bloccate.

- **Enable Traveler client access**: Selezionare questa casella di controllo solamente se si desidera autorizzare l'accesso ai client di IBM Notes Traveler da dispositivi non iOS.

8. Dopo aver inserito le informazioni relative all'istanza, cliccare su **Add** per aggiungere l'istanza all'elenco **Instances**.

   Per ciascuna istanza di proxy, il programma di installazione creerà un certificato che dovrà essere caricato sul server di Sophos Mobile. Una volta cliccato su **Add**, comparirà una finestra di messaggio che descriverà come procedere per caricare il certificato.
9. Nella finestra di messaggio, cliccare su **OK**.
   Si aprirà una finestra di dialogo che mostra la cartella nella quale è stato creato il certificato.

   Nota
   Questa finestra di dialogo può essere aperta anche selezionando l'istanza desiderata e cliccando sul link **Export config and upload to Sophos Mobile server** nella pagina **EAS Proxy instance setup**.

10. Prendere nota della cartella del certificato. Questa informazione verrà richiesta in seguito, al momento di caricare il certificato su Sophos Mobile.
11. Richiesto: Cliccare nuovamente su **Add** per configurare ulteriori istanze del proxy EAS.
12. Una volta configurate tutte le istanze del proxy EAS richieste, cliccare su **Next**.
    Si procederà quindi al test delle porte server che sono state inserite, e verranno configurate le regole in entrata per Windows Firewall.
13. La pagina **Allowed mail user agents** consente di specificare i Mail User Agent (ovvero le applicazioni client di posta elettronica) che sono autorizzati a connettersi al proxy EAS. Quando un client si connette al proxy di EAS utilizzando un'applicazione di posta non specificata, la richiesta viene respinta.
    - Selezionare **Allow all mail user agents** per configurare l'assenza di restrizioni.
    - Cliccare su **Only allow the specified mail user agents** e successivamente selezionare un Mail User Agent dall'elenco. Cliccare su **Add** per aggiungere la voce all'elenco di agenti autorizzati. Ripetere questa procedura per tutti i Mail User Agent a cui è consentito connettersi al proxy EAS.
14. Nella pagina **Sophos Mobile EAS Proxy - Configuration Wizard finished**, cliccare su **Finish** per chiudere il Configuration Wizard e tornare al Setup Wizard.
15. Nel Setup Wizard, verificare che la casella di controllo dell'opzione **Start Sophos Mobile EAS Proxy server now** sia selezionata, e successivamente cliccare su **Finish** per completare la configurazione e avviare il proxy di EAS di Sophos Mobile per la prima volta.

Per completare la configurazione del proxy di EAS, caricare su Sophos Mobile i certificati creati per ciascuna istanza del proxy:

16. Accedere a Sophos Mobile Admin.
17. Sotto **Esterno**, cliccare su **Carica un file**. Caricare il certificato creato dalla procedura guidata per la connessione PowerShell.

    Se è stata impostata più di un'istanza, ripetere questa procedura per i certificati di tutte le istanze.
18. Cliccare su **Salva**.
19. In Windows, aprire la finestra di dialogo **Servizi** e riavviare il servizio **EASProxy**.

Si conclude così l'impostazione iniziale del proxy EAS standalone.

Nota

Ogni giorno, le voci di log del proxy EAS vengono trasferite su un nuovo file, utilizzando il pattern `EASProxy.log.aaaa-mm-gg` per il nome. Questi file di log quotidiano non vengono eliminati automaticamente, per cui col passare del tempo possono causare problemi di spazio disponibile su disco. Si consiglia di impostare un processo che trasferisca i file di log su un percorso di backup.

9.3 Impostazione del controllo dell'accesso alle e-mail tramite PowerShell

È possibile impostare una connessione PowerShell a un server di Exchange oppure Office 365. In questo modo, il servizio proxy EAS comunicherà con il server di posta tramite PowerShell per controllare l'accesso alle e-mail dei dispositivi gestiti. Il traffico e-mail verrà inviato direttamente dai dispositivi al server di posta. Non sarà reindirizzato tramite proxy.

Nota

Poiché macOS non supporta il protocollo ActiveSync, non è possibile utilizzare PowerShell per controllare l'accesso alle e-mail dai Mac.

Lo scenario che prevede l'uso di PowerShell presenta i seguenti vantaggi:

- I dispositivi comunicano direttamente con il server di Exchange.
- Non occorre aprire sul server una porta dedicata al traffico e-mail in entrata proveniente dai dispositivi gestiti.

I server di posta supportati sono:

- Exchange Server 2013
- Exchange Server 2016
- Office 365 con piano Exchange Online

Per il setup di PowerShell:

1. Configurare PowerShell.
2. Creare un account di servizio sul server di Exchange o in Office 365. Questo account verrà utilizzato da Sophos Mobile per eseguire comandi PowerShell.
3. Impostare una o più istanze di connessione PowerShell a Exchange oppure Office 365.
4. Caricare i certificati delle istanze su Sophos Mobile.

Configurazione di PowerShell

1. Nel computer sul quale verrà installato il proxy EAS, aprire Windows PowerShell come amministratore e inserire:

```
PS C:\Windows\system32> Set-ExecutionPolicy RemoteSigned
```

Nota
Se PowerShell non fosse disponibile, effettuarne l'installazione come indicato nell'articolo Installazione di Windows PowerShell (link esterno) di Microsoft.

2. Se si desidera effettuare la connessione a un server di Exchange locale, aprire Windows PowerShell come amministratore sul computer interessato e inserire lo stesso comando indicato in precedenza:

```
PS C:\Windows\system32> Set-ExecutionPolicy RemoteSigned
```

Nota
Questo passaggio non è richiesto per Office 365.

Creazione di un account di servizio

3. Accedere alla console di amministrazione richiesta:
   - Per Exchange Server 2010 SP2: **Console di gestione di Exchange**
   - Per Exchange Server 2013/2016: **Interfaccia di amministrazione di Exchange**
   - Per Office 365: **Interfaccia di amministrazione di Office 365**
4. Creare un account utente. Questo account verrà utilizzato da Sophos Mobile come account di servizio, per eseguire comandi PowerShell.
   - Adoperare un nome utente, come ad es. `smc_powershell`, che identifichi lo scopo dell'account.
   - Disattivare l'impostazione che prevede la modifica della password da parte dell'utente all'accesso successivo.
   - Rimuovere eventuali licenze Office 365 automaticamente assegnate al nuovo account. Gli account di servizio non richiedono alcuna licenza.
5. Creare un nuovo gruppo di ruoli e assegnarvi le autorizzazioni richieste.
   - Adoperare un nome per il gruppo di ruoli quale ad es. `smc_powershell`.
   - Aggiungere i ruoli **Mail Recipients** e **Organization Client Access**.
   - Aggiungere l'account di servizio come membro.

Impostazione delle connessioni PowerShell

6. Utilizzare la procedura guidata come se si desiderasse impostare un proxy di EAS standalone. Nel passaggio della procedura intitolato **EAS Proxy instance setup**, configurare le due seguenti impostazioni:
   - **Instance type**: Selezionare **PowerShell Exchange/Office 365**.
   - **Instance name**: Un nome che identifica l'istanza.
   - **Exchange server**: Il nome o indirizzo IP del server di Exchange (per un'installazione locale del server di Exchange), oppure `outlook.office365.com` (per Office 365). Non includere un prefisso `https://` o un suffisso `/powershell`. Verranno aggiunti automaticamente.
   - **Allow all certificates**: Il certificato presentato dal server di Exchange non sarà verificato. Utilizzare questa opzione se ad esempio nel server di Exchange è installato un certificato

autofirmato. Poiché l'opzione **Allow all certificates** diminuisce il livello di sicurezza della comunicazione del server, si consiglia vivamente di selezionarla solamente se richiesta dall'ambiente di rete.

- **Allow EWS subscription requests from Secure Email**: Selezionare questa opzione per consentire alla app Sophos Secure Email su iOS di effettuare la sottoscrizione alle notifiche push tramite Exchange Web Services (EWS). Le notifiche push informano il dispositivo quando sono presenti messaggi per Secure Email.

Nota

Per impostazione predefinita, il proxy di EAS blocca tutte le richieste rivolte all'interfaccia EWS del server di Exchange; ciò è per questioni di sicurezza. Selezionando questa casella di controllo, verranno autorizzate le richieste di sottoscrizione. Le altre richieste rimarranno bloccate.

- **Service account**: Il nome dell'account utente creato nella console di amministrazione di Exchange oppure Office 365.
- **Password**: La password dell'account utente.

7. Cliccare su **Add** per aggiungere l'istanza all'elenco **Instances**.
8. **Opzionale:** Ripetere i passaggi di cui sopra per impostare connessioni PowerShell ad altri server di Exchange oppure Office 365.
9. Completare la procedura guidata di installazione come descritto in Installazione del proxy EAS standalone (pagina 13).

Caricamento di certificati

10. Accedere a Sophos Mobile Admin.
11. Nella barra laterale dei menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Impostazione del sistema** e successivamente sulla scheda **Proxy EAS**.
12. Richiesto: In **Generale**, selezionare **Limita a Sophos Secure Email** per limitare l'accesso alle e-mail all'app Sophos Secure Email, disponibile per Android e iOS.

    Questa azione impedisce ad altre app di posta elettronica di connettersi al server di posta.
13. Sotto **Esterno**, cliccare su **Carica un file**. Caricare il certificato creato dalla procedura guidata per la connessione PowerShell.

    Se è stata impostata più di un'istanza, ripetere questa procedura per i certificati di tutte le istanze.
14. Cliccare su **Salva**.
15. In Windows, aprire la finestra di dialogo **Servizi** e riavviare il servizio **EASProxy**.

Si conclude così il setup iniziale delle connessioni PowerShell. Il traffico e-mail tra un dispositivo gestito e i server di Exchange oppure Office 365 verrà bloccato se il dispositivo viola una delle regole di conformità. È possibile bloccare un singolo dispositivo impostando su **Nega** la modalità di accesso alle e-mail del dispositivo in questione.

Nota

A seconda della configurazione del server di Exchange, i dispositivi riceveranno una notifica dopo il blocco dell'accesso alle e-mail.

9.4 Configurazione di una connessione al server proxy EAS interno

1. Nella barra laterale dei menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Impostazione del sistema** e successivamente sulla scheda **Proxy EAS**.
2. Richiesto: In **Generale**, selezionare **Limita a Sophos Secure Email** per limitare l'accesso alle e-mail all'app Sophos Secure Email, disponibile per Android e iOS.

   Questa azione impedisce ad altre app di posta elettronica di connettersi al server di posta.
3. Sotto **Interno**, inserire l'URL del server di Exchange o groupware all'interno del campo di testo **Exchange/groupware server URL**.
4. Selezionare **Utilizza SSL/TLS** per adoperare una connessione sicura.
5. Selezionare **Consenti richieste di sottoscrizione ai Servizi Web Exchange da Secure Email** per consentire all'app Sophos Secure Email su iOS di effettuare la sottoscrizione alle notifiche push tramite Exchange Web Services (EWS). Le notifiche push informano il dispositivo quando sono presenti messaggi per Secure Email.

   Per impostazione predefinita, il proxy di EAS blocca tutte le richieste rivolte all'interfaccia EWS del server di Exchange; ciò è per questioni di sicurezza. Selezionando questa casella di controllo, verranno autorizzate le richieste di sottoscrizione. Le altre richieste rimarranno bloccate.
6. Cliccare su **Verifica connessione** per effettuare il test della connessione.
   Verrà visualizzato un messaggio nel caso in cui non sia possibile accedere al server.
7. Cliccare su **Salva**.

9.5 Configurazione di una connessione al server proxy EAS standalone

Per configurare la connessione tra Sophos Mobile e il proxy EAS standalone, occorre caricare il certificato del server proxy di EAS su Sophos Mobile. Questo certificato è stato generato durante la configurazione dell'istanza del proxy EAS.

Importante
Se il servizio proxy EAS viene avviato prima di aver caricato il certificato, Sophos Mobile rifiuterà la connessione al server, e il servizio non si avvierà.

Per caricare il certificato del proxy EAS standalone:

1. Nella barra laterale dei menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Impostazione del sistema** e successivamente sulla scheda **Proxy EAS**.
2. Richiesto: In **Generale**, selezionare **Limita a Sophos Secure Email** per limitare l'accesso alle e-mail all'app Sophos Secure Email, disponibile per Android e iOS.

   Questa azione impedisce ad altre app di posta elettronica di connettersi al server di posta.
3. In **Esterno**, cliccare su **Carica file** e cercare il file del certificato.

   Se è stata impostata più di un'istanza del proxy EAS, ripetere questa procedura per tutte le istanze.
4. Cliccare su **Salva**.

5. In Windows, aprire la finestra di dialogo **Servizi** e riavviare il servizio **EASProxy**.

10 Configurazione di Network Access Control (controllo dell'accesso alla rete)

Sophos Mobile include un'interfaccia per i sistemi di Network Access Control (NAC) di altri vendor. Configurando le connessioni ai sistemi di NAC, se ne concede il permesso di ottenere un elenco di dispositivi e dei relativi stati di conformità. Inoltre, configurando Network Access Control come descritto in questa sezione, è possibile definire in un secondo momento un criterio di conformità che vieti l'accesso alla rete agli utenti che violano regole di conformità specifiche.

Per informazioni su come definire i criteri di conformità, consultare la Guida in linea per amministratori di Sophos Mobile.

Per configurare Network Access Control:

1. Nella barra laterale dei menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Impostazione del sistema**, e successivamente cliccare sulla scheda **Network Access Control**.
2. Selezionare una delle opzioni di integrazione di NAC disponibili nell'elenco:

   - **Sophos UTM**

     Questa opzione abilita l'integrazione di Sophos UTM (versione 9.2 e superiore). Per l'integrazione occorre impostare l'URL del server di SMC e le credenziali dell'utente amministratore nell'interfaccia WebAdmin di Sophos UTM, sotto **Gestione > Sophos Mobile**. Per informazioni dettagliate, consultare la *Guida all'amministrazione di Sophos UTM*.

   - **Cisco ISE**

     Questa opzione abilita l'integrazione di Cisco ISE. Configurare le seguenti impostazioni:

Nome utente	Il nome utente che deve essere specificato in Cisco ISE. Verrà usato da Cisco ISE per accedere a Sophos Mobile.
Password	Inserire una password per effettuare l'accesso a Sophos Mobile.
Conferma password	Ripetere la password.
Pagina di reindirizzamento per i dispositivi bloccati	Un URL verso il quale vengono reindirizzati i dispositivi se non sono autorizzati ad accedere alla rete. Si consiglia di utilizzare l'URL del portale self-service, oppure una pagina informativa con un link al portale self-service.

     In Cisco ISE occorre configurare le impostazioni applicabili, in modo tale che, quando si effettua la connessione all'interfaccia di NAC, vengano utilizzati l'URL del server di Sophos Mobile e le credenziali inserite in questi campi.

   - **Check Point**

     Questa opzione consente l'integrazione di Check Point (versione R77.10 e superiore). Configurare le seguenti impostazioni:

Nome utente	Il nome utente che deve essere specificato in Check Point. Verrà usato da Check Point per accedere a Sophos Mobile.

Password	Inserire una password per effettuare l'accesso a Sophos Mobile.
Conferma password	Ripetere la password.

Nel Mobile Access Gateway di Check Point, occorre configurare alcune impostazioni specifiche, come indicato nell'articolo del Check Point Support Center Implementazione cooperativa del MDM per i client dei dispositivi mobili (in inglese).

- **Servizio web**

  Questa opzione consente di connettere il sistema NAC di un altro vendor all'interfaccia del servizio web.

  Sophos Mobile offre un'interfaccia per il servizio web RESTful che fornisce gli indirizzi MAC e lo stato di accesso alla rete dei dispositivi gestiti.

  È possibile connettere il sistema NAC di un altro vendor a questa interfaccia, utilizzando le credenziali di accesso dell'account di un amministratore di Sophos Mobile.

  Per dettagli specifici sull'implementazione dell'interfaccia del servizio web, consultare la Guida all'interfaccia di Sophos Mobile per Network Access Control.

- **Personalizza**

  Questa opzione consente di configurare l'accesso all'interfaccia NAC basato sul certificato.

  Nota
  L'opzione legacy **Personalizza** è obsoleta e verrà rimossa in una delle prossime release. Utilizzare al suo posto l'opzione **Servizio web** per connettere il sistema NAC di un altro vendor a Sophos Mobile.

  Cliccare su **Carica file** e cercare il certificato del sistema NAC dell'altro vendor. Il certificato viene caricato e visualizzato in una tabella.

  Un sistema NAC di terzi che presenta il certificato al server di Sophos Mobile potrà accedere all'interfaccia di NAC.

3. Nella scheda **Network Access Control**, cliccare su **Salva**.

11 Criteri di conformità

Con i criteri di conformità è possibile:

- Autorizzare, vietare o implementare funzionalità specifiche in un dispositivo.
- Definire le azioni da eseguire quando viene violata una regola di conformità.

È possibile creare criteri di conformità diversi, per poi assegnarli ai gruppi di dispositivi. Ciò consente di applicare livelli di protezione diversi ai dispositivi gestiti.

Consiglio
Se si ha intenzione di gestire sia dispositivi aziendali che personali, si consiglia di definire criteri di conformità ben distinti, almeno per quanto riguarda questi due tipi di dispositivi.

11.1 Crea criterio di conformità

1. Nella barra laterale dei menù, sotto **CONFIGURA**, cliccare su **Criteri di conformità**.
2. Nella pagina **Criteri di conformità**, cliccare su **Crea criterio di conformità** e successivamente selezionare il modello su cui si desidera sia basato il criterio:
   - **Modello predefinito**: una selezione di regole di conformità, senza azioni definite.
   - **Modello PCI**, **Modello HIPAA**: regole di conformità basate, rispettivamente, sugli standard di sicurezza HIPAA e PCI DSS.

   Il modello selezionato non limita le opzioni di configurazione successive.
3. Inserire un nome e, opzionalmente, una descrizione per il criterio di conformità.

Ripetere la seguente procedura per tutte le piattaforme, a seconda delle esigenze.

4. Verificare che la casella di spunta **Abilita piattaforma** risulti selezionata in tutte le schede.
   Se questa casella non è selezionata, non sarà possibile verificare la conformità dei dispositivi appartenenti alla piattaforma corrispondente.
5. Sotto **Regola**, configurare le regole di conformità per la piattaforma selezionata.
   Per una descrizione delle regole disponibili per ciascun tipo di dispositivo, cliccare su **?** nell'intestazione della pagina.

Nota
Ciascuna regola di conformità possiede un livello di gravità fisso (alto, medio, basso), che viene segnalato da un'icona blu. Il livello di gravità aiuta a valutare l'importanza di ciascuna regola e le azioni da implementare in caso di violazione.

Nota
Per i dispositivi nei quali Sophos Mobile gestisce il contenitore Sophos e non il dispositivo intero, è applicabile un solo sotto-set di regole di conformità. Sotto **Evidenzia regole**, selezionare un tipo di gestione che evidenzi le regole applicabili.

6. Sotto **Se viene violata una regola**, definire le azioni da intraprendere in caso di violazione di una regola:

Opzione	Descrizione
Nega e-mail	Vieta accesso alle e-mail Questa azione può essere effettuata solamente se è stata configurata una connessione al proxy EAS standalone. Vedere Configurazione di una connessione al server proxy EAS standalone (pagina 19). Questa azione è disponibile solamente per i dispositivi Android, iOS, Windows e Windows Mobile.
Blocca contenitore	Disattiva le app Sophos Secure Workspace e Secure Email. Ciò incide sui documenti, le e-mail e l'accesso al web gestiti da queste app. Questa azione può essere effettuata solamente dopo l'attivazione di una licenza Mobile Advanced. Questa azione è disponibile solamente per i dispositivi Android e iOS.
Nega rete	Vieta accesso alla rete Questa azione può essere effettuata solamente se è stato configurato Network Access Control (controllo dell'accesso alla rete). Vedere Configurazione di Network Access Control (controllo dell'accesso alla rete) (pagina 21).
Crea avviso	Crea un avviso. Gli avvisi sono visualizzati nella pagina **Avvisi**.
Trasferisci bundle delle operazioni	Trasferisce un bundle delle operazioni specifico al dispositivo. Questa azione è disponibile solamente per i dispositivi Android, iOS, macOS e Windows. Si consiglia per il momento di impostare questa opzione su **Nessuno**. Per ulteriori informazioni, consultare la Guida in linea per amministratori di Sophos Mobile. **Importante** Se utilizzati in modo improprio, i bundle delle operazioni potrebbero essere configurati in modo errato o potrebbero addirittura portare alla cancellazione dei dati dal dispositivo. Per assegnare i bundle delle operazioni corretti alle regole di conformità, è necessaria una conoscenza approfondita del sistema.

7. Una volta specificate le impostazioni per tutte le piattaforme richieste, cliccare su **Salva** per salvare il criterio di conformità con il nome indicato.
Il nuovo criterio di conformità viene visualizzato nella pagina **Criteri di conformità**.

Per utilizzare un criterio di conformità, assegnare il criterio a un gruppo di dispositivi. Questa procedura viene descritta nella sezione successiva.

12 Gruppi di dispositivi

I gruppi di dispositivi vengono utilizzati per categorizzare i dispositivi. Permettono di gestire i dispositivi in maniera efficace, in quanto prevedono l'esecuzione delle operazioni su un gruppo, per evitare di doverle ripetere per ciascun singolo dispositivo.

Un dispositivo appartiene sempre a un gruppo di dispositivi. È possibile assegnare un dispositivo a un gruppo di dispositivi durante la sua aggiunta a Sophos Mobile.

Consiglio

Unire nello stesso gruppo solo dispositivi con lo stesso sistema operativo. Ciò semplificherà l'uso dei gruppi per le attività di installazione e per altre operazioni specifiche del sistema operativo.

12.1 Crea gruppo di dispositivi

1. Nella barra laterale del menù, sotto **GESTISCI**, cliccare su **Gruppi dispositivi**, e successivamente su **Crea gruppo di dispositivi**.
2. Nella pagina **Modifica il gruppo di dispositivi**, inserire un nome e una descrizione per il nuovo gruppo di dispositivi.
3. Nell'opzione **Criteri di conformità**, selezionare i criteri di conformità da applicare a dispositivi aziendali e personali.
4. Cliccare su **Salva**.

Nota

Le impostazioni del gruppo di dispositivi includono l'opzione **Consenti la registrazione automatica per iOS**. Questa opzione consente di effettuare la registrazione dei dispositivi iOS all'Apple Configurator. Per ulteriori informazioni, consultare la Guida in linea per amministratori di Sophos Mobile.

Il nuovo gruppo verrà così creato e visualizzato nella pagina **Gruppi di dispositivi**.

13 Configurazione dei dispositivi iOS

13.1 Creazione di un profilo per dispositivi iOS

Questa sezione descrive la creazione di un profilo per la configurazione iniziale dei dispositivi iOS.

Si consiglia di impostare profili separati per:

- Criteri e restrizioni della password
- Impostazioni di account per Exchange (se richiesto)
- Impostazioni VPN (se richiesto)
- Impostazioni Wi-Fi (se richiesto)
- Certificati root e client (se richiesto)

Nota

Sophos Mobile offre due metodi per creare profili per i dispositivi iOS:

- Creazione dei profili direttamente da Sophos Mobile Admin.
- Importazione dei profili creati con Apple Configurator.

Questa sezione descrive come creare profili in Sophos Mobile Admin. Per informazioni su come importare i profili creati utilizzando Apple Configurator, consultare la Guida in linea per amministratori di Sophos Mobile.

Per creare il profilo di un dispositivo iOS per criteri e restrizioni della password:

1. Nella barra laterale dei menù, sotto **CONFIGURA**, cliccare su **Profili, criteri > iOS**.
2. Nella pagina **Profili e criteri**, cliccare su **Crea > Profilo del dispositivo**.
3. Nella pagina **Modifica profilo**, configurare le seguenti impostazioni:
   a) **Nome**: Inserire un nome per il profilo. Si consiglia di utilizzare il nome `Profilo SSP iOS` per i profili applicati durante la registrazione tramite portale self-service (Self-Service Portal, SSP).
   b) **Azienda**: Inserire il nome dell'organizzazione da assegnare al profilo, ad esempio il nome di un'azienda.
   c) **Descrizione**: Inserire una descrizione per il profilo, ad esempio `profilo di base`.
4. Per aggiungere criteri per la password al profilo, cliccare su **Aggiungi configurazione**, selezionare **Criteri password**.
5. Nella pagina **Criteri password**, configurare le necessarie impostazioni per la password.
   Per una descrizione dettagliata delle impostazioni, cliccare su **?** nell'intestazione della pagina.
6. Per salvare le impostazioni, cliccare su **Applica**.
   La configurazione dei **Criteri password** viene visualizzata nella pagina **Modifica profilo**, sotto **Configurazioni**.
7. Per aggiungere restrizioni, cliccare su **Aggiungi configurazione**, selezionare **Restrizioni**.
8. Nella pagina **Restrizioni**, selezionare la restrizione richiesta.

   Alcune restrizioni richiedono tipi di dispositivo o versioni di iOS specifici. Questi requisiti vengono visualizzati sulla destra, accanto a ciascuna restrizione.

   Per una descrizione dettagliata delle impostazioni, cliccare su **?** nell'intestazione della pagina.

9. Per salvare le impostazioni, cliccare su **Applica**.
   La configurazione delle **Restrizioni** viene visualizzata nella pagina **Modifica profilo**, sotto **Configurazioni**.
10. Nella pagina **Modifica profilo**, cliccare su **Salva** per salvare il profilo.

Il profilo viene visualizzato nella pagina **Profili e criteri** ed è disponibile per essere trasferito sui dispositivi iOS.

All'occorrenza, creare profili aggiuntivi per: impostazioni di account per Exchange, impostazioni VPN, impostazioni Wi-Fi e installazione di certificati root e client.

13.2 Creazione di un bundle delle operazioni per profili iOS

1. Nella barra laterale dei menù, sotto **CONFIGURA**, cliccare su **Bundle delle operazioni > iOS**.
2. Nella pagina **Bundle delle operazioni**, cliccare su **Crea bundle delle operazioni**.
   Verrà visualizzata la pagina **Modifica bundle delle operazioni**.
3. Inserire nei campi corrispondenti nome e, opzionalmente, una descrizione per il nuovo bundle delle operazioni.

   Il numero della versione viene incrementato automaticamente a ogni salvataggio del bundle delle operazioni.
4. Richiesto: Selezionare **Selezionabile per effettuare azioni di conformità** per trasferire il bundle delle operazioni su un dispositivo, quando viola una regola di conformità. Vedere Criteri di conformità (pagina 23).

   Nota
   Questa opzione è disattivata durante la modifica di bundle delle operazioni esistenti, o nel caso in cui il bundle delle operazioni sia già utilizzato per effettuare azioni di conformità.
5. Richiesto: Per i bundle delle operazioni iOS, selezionare **Ignora errori di installazione delle app** per procedere all'elaborazione del bundle delle operazioni anche se non dovesse essere possibile installare un'app.

   Questa opzione è disattivata quando il bundle delle operazioni non contiene alcuna operazione **Installa app**.
6. Cliccare su **Crea operazione**, selezionare **Registrati** e inserire un nome per l'operazione. Cliccare su **Applica** per creare l'operazione.

   È possibile modificare l'ordine di installazione delle operazioni utilizzando le frecce di ordinamento nella parte destra dell'elenco delle operazioni.
7. Cliccare nuovamente su **Crea operazione** e selezionare **Installa profilo o assegna criterio**. Attribuire all'operazione un nome significativo, ad esempio `Installa profilo per i criteri della password`, e selezionare il profilo creato. Cliccare su **Applica** per creare l'operazione.
8. Se sono stati configurati profili per le impostazioni di Exchange, VPN o Wi-Fi, ripetere questo passaggio per ciascun profilo.
9. Richiesto: Aggiungere altre operazioni al bundle delle operazioni.

Consiglio
È possibile modificare l'ordine di installazione delle operazioni utilizzando le frecce di ordinamento nella parte destra dell'elenco delle operazioni.

10. Una volta aggiunte tutte le operazioni necessarie al bundle delle operazioni, cliccare su **Salva** nella pagina **Modifica bundle delle operazioni**.

Il bundle delle operazioni sarà ora disponibile per il trasferimento e verrà visualizzato nella pagina **Bundle delle operazioni**.

14 Configurazione dei dispositivi Android

14.1 Creazione di un profilo per dispositivi Android

In questa sezione si descrive la creazione di un profilo per la configurazione iniziale dei dispositivi Android.

Si consiglia di impostare profili separati per:

- Criteri e restrizioni della password
- Impostazioni di account per Exchange (se richiesto)
- Impostazioni VPN (se richiesto)
- Impostazioni Wi-Fi (se richiesto)
- Certificati root e client (se richiesto)

1. Nella barra laterale del menù, sotto **CONFIGURA**, cliccare su **Profili, criteri > Android**.
2. Nella pagina **Profili e criteri**, cliccare su **Crea > Profilo del dispositivo**.
3. Nella pagina **Modifica profilo**, configurare le seguenti impostazioni:
   a) **Nome**: Inserire un nome per il profilo. Si consiglia di utilizzare il nome `Profilo SSP Android` per i profili applicati durante la registrazione tramite Portale self-service.
   b) Richiesto: **Descrizione**: Inserire una descrizione per il profilo, ad esempio `profilo di base`.
4. Per aggiungere criteri per la password al profilo, cliccare su **Aggiungi configurazione**, selezionare **Criteri password**.
   Viene visualizzata la pagina **Criteri password**.
5. Sotto **Tipo di password**, indicare il tipo di password che si desidera definire, ad esempio **Complesso**.
6. Configurare le impostazioni della password richieste.
   Le impostazioni disponibili dipendono dal tipo di password selezionato. Per una descrizione dettagliata de tutte le impostazioni, cliccare su **?** nell'intestazione della pagina.
7. Per salvare le impostazioni, cliccare su **Applica**.
   La configurazione dei **Criteri password** viene visualizzata nella pagina **Modifica profilo**, sotto **Configurazioni**.
8. Per aggiungere restrizioni, cliccare su **Aggiungi configurazione**, selezionare **Restrizioni**.
9. Nella pagina **Restrizioni**, selezionare la restrizione richiesta.
   Alcune restrizioni richiedono tipi di dispositivo o versioni di Android specifici. Questi requisiti vengono visualizzati sulla destra, accanto a ciascuna restrizione.
   Per una descrizione dettagliata delle impostazioni, cliccare su **?** nell'intestazione della pagina.
10. Per salvare le impostazioni, cliccare su **Applica**.
    La configurazione delle **Restrizioni** viene visualizzata nella pagina **Modifica profilo**, sotto **Configurazioni**.
11. Nella pagina **Modifica profilo**, cliccare su **Salva** per salvare il profilo.

Il profilo viene visualizzato nella pagina **Profili e criteri**, ed è disponibile per essere trasferito sui dispositivi Android.

All'occorrenza, creare profili aggiuntivi per: impostazioni di account per Exchange, impostazioni VPN, impostazioni Wi-Fi e installazione di certificati root e client.

14.2 Creazione di un bundle delle operazioni per dispositivi Android

1. Nella barra laterale del menù, sotto **CONFIGURA**, cliccare su **Bundle delle operazioni > Android**.
2. Nella pagina **Bundle delle operazioni**, cliccare su **Crea bundle delle operazioni**.
   Verrà visualizzata la pagina **Modifica bundle delle operazioni**.
3. Inserire nei campi corrispondenti nome e, opzionalmente, una descrizione per il nuovo bundle delle operazioni.

   Il numero della versione viene incrementato automaticamente a ogni salvataggio del bundle delle operazioni.
4. Richiesto: Selezionare **Selezionabile per effettuare azioni di conformità** per trasferire il bundle delle operazioni su un dispositivo, quando viola una regola di conformità. Vedere Criteri di conformità (pagina 23).

   Nota
   Questa opzione è disattivata durante la modifica di bundle delle operazioni esistenti, o nel caso in cui il bundle delle operazioni sia già utilizzato per effettuare azioni di conformità.
5. Richiesto: Per i bundle delle operazioni iOS, selezionare **Ignora errori di installazione delle app** per procedere all'elaborazione del bundle delle operazioni anche se non dovesse essere possibile installare un'app.

   Questa opzione è disattivata quando il bundle delle operazioni non contiene alcuna operazione **Installa app**.
6. Cliccare su **Crea operazione**, selezionare **Registrati** e inserire un nome per l'operazione. Cliccare su **Applica** per creare l'operazione.

   È possibile modificare l'ordine di installazione delle operazioni utilizzando le frecce di ordinamento nella parte destra dell'elenco delle operazioni.
7. Cliccare nuovamente su **Crea operazione** e selezionare **Installa profilo o assegna criterio**. Attribuire all'operazione un nome significativo, ad esempio `Installa profilo per i criteri della password`, e selezionare il profilo creato. Cliccare su **Applica** per creare l'operazione.
8. Se sono stati configurati profili per le impostazioni di Exchange, VPN o Wi-Fi, ripetere questo passaggio per ciascun profilo.
9. Richiesto: Aggiungere altre operazioni al bundle delle operazioni.

   Consiglio
   È possibile modificare l'ordine di installazione delle operazioni utilizzando le frecce di ordinamento nella parte destra dell'elenco delle operazioni.
10. Una volta aggiunte tutte le operazioni necessarie al bundle delle operazioni, cliccare su **Salva** nella pagina **Modifica bundle delle operazioni**.

Il bundle delle operazioni sarà ora disponibile per il trasferimento e verrà visualizzato nella pagina **Bundle delle operazioni**.

15 Aggiornamento delle impostazioni del portale self-service

Una volta creati bundle delle operazioni da trasferire quando gli utenti registrano i propri dispositivi nel portale self-service, occorre aggiornare le impostazioni del portale self-service con le necessarie impostazioni di gruppo:

1. Nella barra laterale del menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Portale self-service**, e successivamente cliccare sulla scheda **Impostazioni gruppo**.
2. Cliccare sull'impostazione del gruppo **Predefinita**.
   Si aprirà la finestra di dialogo **Modifica impostazioni gruppo**.
3. Negli elenchi **Pacchetto iniziale - dispositivi aziendali** e **Pacchetto iniziale - dispositivi personali**, selezionare i bundle delle operazioni creati per i dispositivi Android e iOS.
4. Selezionare la casella di spunta **Attiva** per le piattaforme che si desidera rendere disponibili nel portale self-service:
5. Nell'elenco **Aggiungi al gruppo di dispositivi**, selezionare il gruppo al quale saranno aggiunti i dispositivi quando ne viene effettuata la registrazione nel portale self-service.
6. Cliccare su **Applica**.
7. Nella scheda **Impostazioni gruppo**, cliccare su **Salva**.

16 Configurazione della gestione degli utenti

Sophos Mobile offre due metodi diversi per gestire gli account utenti per Sophos Mobile Admin e il portale self-service:

- Con la **gestione degli utenti interni** è possibile creare utenti aggiungendoli manualmente da Sophos Mobile Admin, oppure importandoli da un file con valori delimitati da virgole (CSV).
- Con la **gestione degli utenti esterni**, è possibile effettuare la connessione a una directory LDAP già esistente, e assegnare i dispositivi a gruppi e profili in base alla loro appartenenza a una directory.

Nota

- Non è possibile cambiare metodo di gestione degli utenti una volta che i dispositivi sono stati assegnati agli utenti.
- Per la gestione degli utenti esterni, deve essere disponibile un ambiente LDAPS (LDAP su SSL/TLS). Sophos Mobile si connette al server LDAP utilizzando la porta LDAPS numero 636.

Per selezionare il metodo di gestione degli utenti:

1. Nella barra laterale dei menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Impostazione del sistema**, e successivamente cliccare sulla scheda **Impostazione utente**.
2. Selezionare l'origine dei dati degli account per Sophos Mobile Admin e il portale self-service (SSP):
   - Selezionare **Directory interna** per utilizzare la gestione utenti interni.
   - Selezionare **Directory LDAP esterna** per adoperare la gestione degli utenti esterni invece di o in combinazione con la gestione degli utenti interni.
3. Se è stata selezionata **Directory LDAP esterna**, cliccare su **Configura LDAP esterno** per specificare i dettagli del server. Vedere Configurazione della connessione a una directory esterna (pagina 35).
4. Cliccare su **Salva**.

Nota

Una volta salvate le impostazioni, nella scheda **Impostazione utente** sarà disponibile solamente il metodo di gestione degli utenti selezionato. Per modificare questa selezione in un secondo momento, selezionare **Nessuno** e salvare. Selezionare prima **Non è disponibile alcun profilo SSP specifico per l'utente, né alcun amministratore di LDAP.** per rendere nuovamente disponibili tutte le opzioni.

17 Utilizzo della gestione utenti interni

17.1 Creazione di un utente di test per il portale self-service

Per testare il provisioning tramite portale self-service, creare un proprio account utente del portale self-service. Questo account verrà utilizzato per accedere al portale self-service e per testare la registrazione dei dispositivi.

Per creare un account utente di test per il portale self-service:

1. Nella barra laterale del menù, sotto **GESTISCI**, cliccare su **Utenti**, e successivamente su **Crea utente**.
2. Configurare i dovuti dettagli dell'account.

   Verificare che il campo **Invia e-mail di registrazione** sia selezionato.
3. Cliccare su **Salva**.

L'utente viene aggiunto all'elenco di utenti del portale self-service, e un'e-mail di registrazione viene inviata all'indirizzo e-mail specificato nei dettagli dell'account.

17.2 Test della registrazione del dispositivo tramite portale self-service

Si consiglia di testare la procedura di registrazione tramite portale self-service, prima di mettere il portale self-service a disposizione degli utenti.

Accedere al portale self-service con l'account dell'utente di test creato nella sezione Creazione di un utente di test per il portale self-service (pagina 33), ed effettuare registrazioni di prova per tutte le piattaforme che si desidera gestire con Sophos Mobile.

17.3 Importazione degli utenti su Sophos Mobile

Una volta effettuato il test di registrazione tramite portale self-service, è possibile importare l'elenco degli utenti in Sophos Mobile.

L'importazione degli utenti è applicabile solamente per la gestione degli utenti interni. Per la gestione degli utenti esterni, tutti gli utenti assegnati a un determinato gruppo LDAP possono effettuare l'accesso al sistema.

È possibile aggiungere nuovi utenti del portale self-service importando un file con valori delimitati da virgole (CSV) e con codifica UTF-8 che può includere sino a un massimo di 300 utenti.

Nota
Utilizzare un editor di testo per apportare modifiche al file CSV. Se si utilizza Microsoft Excel, i valori inseriti potrebbero non essere risolti in modo corretto. Verificare che il file venga salvato con l'estensione `.csv`.

Consiglio
Un file di esempio, in cui vengono riportati i nomi e l'ordine corretto delle colonne, è scaricabile dalla pagina **Importa utenti**.

Per importare gli utenti da un file CSV:

1. Nella barra laterale del menù, sotto **GESTISCI**, cliccare su **Utenti**, e successivamente su **Importa utenti**.
2. Nella pagina **Importa utenti**, selezionare **Invia e-mail di registrazione**.
3. Cliccare su **Carica file** e navigare sul file CSV preparato in precedenza.
   Le voci verranno lette dal file e visualizzate.
4. Se i dati non vengono impostati nel giusto formato, o se sono inconsistenti, non sarà possibile importare l'intero file. In tale eventualità, esaminare i messaggi di errore visualizzati accanto alle relative voci, correggere il contenuto del file CSV a seconda di quanto richiesto e caricarlo nuovamente.
5. Cliccare su **Fine** per creare gli account utente.

Gli utenti verranno importati e visualizzati nella pagina **Mostra utenti**. Riceveranno le e-mail con le credenziali di accesso per il portale self-service.

18 Utilizzo della gestione utenti esterni

18.1 Configurazione della connessione a una directory esterna

Quando si configura una directory LDAP esterna per la gestione degli account degli utenti per Sophos Mobile Admin e il portale self-service, occorre configurare la connessione della directory in modo tale che Sophos Mobile possa recuperare i dati degli utenti dal server LDAP.

Nota

Non viene effettuata alcuna sincronizzazione tra la directory LDAP e Sophos Mobile. Sophos Mobile accede alla directory LDAP solamente per cercare informazioni sugli utenti. Eventuali modifiche a un account utente LDAP non verranno implementate nel database di Sophos Mobile, e viceversa.

1. Nella barra laterale dei menù, sotto **IMPOSTAZIONI**, cliccare su **Impostazione > Impostazione del sistema**, e successivamente cliccare sulla scheda **Impostazione utente**.
2. Selezionare **Directory LDAP esterna**.
3. Cliccare su **Configura LDAP esterno** per specificare i dettagli del server.
4. Nella pagina **Dettagli server**, configurare le seguenti impostazioni:
   a) Nel campo **Tipo LDAP**, selezionare il tipo di server LDAP:
      - **Active Directory**
      - **IBM Domino**
      - **NetIQ eDirectory**
      - **Red Hat Directory Server**
      - **Zimbra**

   b) Nel campo **URL principale**, inserire l'URL del server di directory principale. È possibile inserire l'IP o il nome del server. Selezionare **SSL/TLS** per proteggere la connessione del server con SSL o TLS (a seconda della compatibilità del server). L'opzione **SSL/TLS** non può essere deselezionata per Sophos Mobile as a Service.

   c) Richiesto: Nel campo **URL secondario**, inserire l'URL di un server di directory da adoperare come fallback nell'eventualità in cui il server primario sia impossibile da raggiungere.
   È possibile inserire l'IP o il nome del server. Selezionare **SSL/TLS** per proteggere la connessione del server con SSL o TLS (a seconda della compatibilità del server). L'opzione **SSL/TLS** non può essere deselezionata per Sophos Mobile as a Service.

   d) Nel campo **Utente**, inserire un account per le operazioni di ricerca nel server di directory. Sophos Mobile adopera le credenziali dell'account quando effettua la connessione al server di directory.

      Per Active Directory, occorre anche inserire il dominio pertinente. I formati supportati sono:

      - *<Dominio>\<nome utente>*
      - *<Nome utente>@<dominio>.<codice dominio>*

> **Nota**
> Per motivi di sicurezza, si consiglia di specificare per il server di directory un utente che abbia diritti di sola lettura e non di scrittura.

e) Nel campo **Password**, inserire la password relativa all'utente specificato.

Cliccare su **Avanti**.

5. Nella pagina **Base di ricerca**, inserire il nome distinto (ND) dell'oggetto della base di ricerca.
   L'oggetto della base di ricerca definisce il percorso nella directory esterna dal quale comincia la ricerca di un utente o gruppo di utenti.
6. Nella pagina **Campi di ricerca**, definire quali campi della directory debbano essere utilizzati per la risoluzione dei segnaposto *%_USERNAME_%* ed *%_EMAILADDRESS_%* nei profili e nei criteri. Digitare i nomi dei campi richiesti, oppure effettuarne la selezione dagli elenchi **Nome utente** ed **E-mail**.

> **Nota**
> Gli elenchi contengono solamente i campi configurati per l'utente attualmente connesso alla directory LDAP, come specificato nel passaggio 4.d (pagina 35) qui sopra. Se ad esempio un campo e-mail non dovesse essere stato configurato per l'utente in questione, occorrerà inserire manualmente il valore richiesto nel campo **E-mail**.

Nel caso di Active Directory sono applicabili le seguenti associazioni campi:

- **Nome utente**: `sAMAccountName`
- **Nome**: `givenName`
- **Cognome**: `sn`
- **E-mail**: `mail`

7. Nella pagina **Configurazione SSP**, specificare gli utenti a cui è consentito accedere al portale self-service. Inserire le informazioni pertinenti nel campo **Gruppo di directory LDAP**, adoperando una delle seguenti opzioni:

   - Se si inserisce un asterisco `*`, si concederà l'accesso al portale self-service a tutti i membri dei gruppi di directory LDAP.

> **Nota**
> Il valore `*` rappresenta *tutti i gruppi* e non *tutti gli utenti*. Gli utenti che non appartengono ad alcun gruppo di directory LDAP non saranno inclusi.

   - Se si inserisce il nome di un gruppo che è definito nel server di directory, si concederà l'accesso al portale self-service a tutti i membri del gruppo in questione. Una volta inserito il nome del gruppo, cliccare su **Risolvi gruppo** per risolvere il nome del gruppo a un nome distinto (ND).
   - Se il campo viene lasciato vuoto, nessun utente del server di directory potrà accedere al portale self-service. Utilizzare questa opzione se si desidera abilitare la gestione degli utenti esterni per Sophos Mobile Admin ma non per il portale self-service.

> **Nota**
> Il gruppo che viene specificato in questo campo non ha nessuna correlazione con il gruppo utenti che viene definito nella scheda **Impostazioni del gruppo** della pagina **Portale self-service**. Queste altre impostazioni servono per definire i bundle delle operazioni, l'appartenenza al gruppo Sophos Mobile e le piattaforme per dispositivi mobili che sono disponibili per ciascun gruppo utenti.
>
> Per ulteriori informazioni sulle impostazioni per i gruppi del portale self-service, consultare la Guida in linea per amministratori di Sophos Mobile.

8. Cliccare su **Applica**.
9. Nella scheda **Impostazione utente**, cliccare su **Salva**.

18.2 Test della registrazione del dispositivo per gli utenti LDAP

Si consiglia di testare la procedura di registrazione tramite portale self-service, prima di mettere il portale self-service a disposizione degli utenti.

Accedere al portale self-service con le proprie credenziali LDAP, ed effettuare prove di registrazione per tutte le piattaforme che si desidera gestire con Sophos Mobile.

19 Utilizzo della procedura guidata di registrazione del dispositivo per assegnare e registrare nuovi dispositivi

I nuovi dispositivi possono essere registrati in maniera molto semplice, grazie alla procedura guidata di registrazione dei dispositivi. Offre un flusso di lavoro che unisce e combina le seguenti operazioni:

- Aggiunta di un nuovo dispositivo a Sophos Mobile.
- Opzionale: Assegnazione di un utente al dispositivo.
- Registrazione del dispositivo.
- Facoltativa: Trasferisce un bundle delle operazioni al dispositivo.

Per avviare la procedura guidata di registrazione del dispositivo:

1. Nella barra laterale del menù, sotto **GESTISCI**, cliccare su **Dispositivi**, e successivamente su **Aggiungi > Procedura guidata di registrazione**.

> **Consiglio**
> In alternativa, la procedura guidata può essere avviata dalla pagina **Pannello di controllo**, cliccando sul widget **Aggiungi dispositivo**.

2. Nella pagina **Inserisci parametri di ricerca utente** della procedura guidata, è possibile inserire i criteri di ricerca per l'individuazione di un utente a cui assegnare il dispositivo, oppure selezionare **Salta assegnazione utente** per registrare un dispositivo che per il momento non si desidera assegnare ad alcun utente.
3. Una volta inserito un criterio di ricerca, la procedura guidata visualizzerà un elenco di utenti che hanno riscontrato una corrispondenza. Selezionare l'utente desiderato.
4. Nella pagina **Dettagli dispositivo** della procedura guidata, configurare le seguenti impostazioni:

Opzione	Descrizione
Piattaforma	La piattaforma del dispositivo.
Nome	Un nome univoco che contraddistinguerà il dispositivo per la gestione con Sophos Mobile.
Descrizione	Una descrizione opzionale del dispositivo.
Numero telefonico	Un numero di telefono opzionale. Inserire il numero, completo di prefisso internazionale, ad esempio: `+491701234567`.
Indirizzo e-mail	L'indirizzo e-mail a cui inviare le istruzioni per la registrazione. Se per il cliente è configurata la gestione degli utenti, sarà l'indirizzo e-mail dell'utente assegnato al dispositivo. Se non è configurata alcuna gestione degli utenti, immettere un indirizzo e-mail.
Proprietario	Selezionare il tipo di proprietario del dispositivo: **Aziendale** o **Personale**.

Opzione	Descrizione
Gruppo di dispositivi	Selezionare il gruppo a cui verrà assegnato il dispositivo. Se non sono ancora stati creati gruppi di dispositivi, è possibile selezionare il gruppo **Predefinito**, che è sempre disponibile.

5. Selezionare un bundle delle operazioni da trasferire sul dispositivo dopo la registrazione. In alternativa, selezionare **Registra solo il dispositivo** per registrare il dispositivo senza trasferire un bundle delle operazioni.
   Cliccando su **Avanti**, il dispositivo verrà aggiunto a Sophos Mobile.
6. Nella pagina della procedura guidata **Registrazione**, seguire le istruzioni per completare il processo di registrazione.

Nota
Nei Mac, la procedura di registrazione deve essere effettuata dall'utente che sarà gestito da Sophos Mobile. Per installare il profilo di registrazione, l'utente deve immettere una password di amministrazione.

7. Una volta completata la registrazione, cliccare su **Fine** per chiudere la procedura guidata di registrazione del dispositivo.

Nota
- Una volta effettuate tutte le selezioni, è possibile chiudere la procedura guidata senza dover attendere che compaia il pulsante **Fine**. Un'operazione di registrazione verrà così creata ed elaborata in background.

20 Glossario

dispositivo	Il dispositivo da gestire (ad es. smartphone, tablet o dispositivo Windows 10).
registrazione	La registrazione di un dispositivo a Sophos Mobile.
Enterprise App Store	Un archivio di app ospitate sul server di Sophos Mobile. L'amministratore può aggiungere app all'Enterprise App Store utilizzando Sophos Mobile Admin. Gli utenti possono quindi adoperare l'app Sophos Mobile Control per installare le suddette app sui propri dispositivi.
provisioning	Il processo di installazione dell'app Sophos Mobile Control su un dispositivo.
Portale self-service	L'interfaccia web che consente agli utenti di registrare i propri dispositivi ed effettuare altre operazioni senza dover richiedere l'intervento dell'helpdesk.
Licenza Mobile Advanced	Con una licenza di tipo Mobile Advanced è possibile gestire le app Sophos Mobile Security, Sophos Secure Workspace e Sophos Secure Email con Sophos Mobile.
SMSec	Acronimo di Sophos Mobile Security.
Client Sophos Mobile	L'app Sophos Mobile Control installata sui dispositivi gestiti da Sophos Mobile.
Console di Sophos Mobile	L'interfaccia web utilizzata per gestire i dispositivi.
Sophos Mobile Security	Un'app di protezione per i dispositivi Android. Questa app può essere gestita da Sophos Mobile, a patto che si disponga di una licenza Mobile Advanced attiva.
Sophos Secure Email	Un'app per dispositivi Android e iOS che fornisce un contenitore sicuro per la gestione di e-mail, calendario e contatti. Questa app può essere gestita da Sophos Mobile, a patto che si disponga di una licenza Mobile Advanced attiva.
Sophos Secure Workspace	Un'app per dispositivi Android e iOS che offre un'area di lavoro sicura, nella quale gli utenti possono navigare, gestire, modificare, condividere, cifrare e decifrare documenti provenienti da vari provider di servizi di archiviazione, o distribuiti dalla vostra azienda. Questa app può essere gestita da Sophos Mobile, a patto che si disponga di una licenza Mobile Advanced attiva.
bundle delle operazioni	Un pacchetto creato per includere varie operazioni diverse in un'unica transazione.

Sarà possibile unire insieme tutte le operazioni necessarie per completare la registrazione e rendere operativo un dispositivo.

21 Supporto tecnico

È possibile ricevere supporto tecnico per i prodotti Sophos in ciascuno dei seguenti modi:

- Visitando la Sophos Community su community.sophos.com/ e cercando altri utenti che hanno riscontrato lo stesso problema.
- Visitando la knowledge base del supporto Sophos su www.sophos.com/it-it/support.aspx.
- Scaricando la documentazione del prodotto su www.sophos.com/it-it/support/documentation.aspx.
- Aprendo un ticket col team di supporto su https://secure2.sophos.com/it-it/support/contact-support/support-query.aspx.

22 Note legali

Ultimo aggiornamento: 20171212